GTA Georgia Technology Authority	**Georgia Technology Authority**	
Title:	**Information Security – Risk Management**	
PSG Number:	PS-08-031.01	**Topical Area:** Security
Document Type:	Policy	**Pages:** 2
Issue Date:	3/20/08	**Effective Date:** 3/20/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes a requirement for agencies to implement a risk-based approach to cost-effective information security management.	

PURPOSE

"Risk" is the net negative impact of the exploitation of a vulnerability, considering both the probability and the impact of occurrence. "Risk management" is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. An effective risk management process is an important component of a successful IT security program and an essential management function of the organization.

The principal goal of an organization's risk management process is to protect the organization and its ability to perform their mission. It fosters informed decision making, allowing the security management organization to balance the operation and economic costs of protective measures and achieve gains in mission capability.

This policy requires agencies to take a risk-based approach to securing their information systems.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

POLICY

Each agency shall institute an organization-wide risk management approach to information security that assesses the risks (including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction) to information and information systems that support the operations and assets of the organization.

Each agency shall develop policies, procedures and select cost-effective controls (based on the risk assessment) that reduce information security risks to an

acceptable level and ensure information security is addressed throughout the lifecycle of each organization's information systems.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Information Security Infrastructure (Standard)
- Risk Management Framework (Standard)

REFERENCES

- NIST SP 800-12 (chapters 7 & 10) Introduction to Computer Security NIST Handbook
- NIS SP 800-30 Risk Management Guide for Information Technology Systems
- NIST SP 800-65 Integrating IT Security into the Capital Planning and Investments Controls Process

TERMS and DEFINITIONS

Risk – A function of the likelihood of a given threat source exploiting a potential vulnerability, and the resulting impact of that adverse event on the organization.

Risk Management - The process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Note: The PSG number was changed from P-08-031.01 on September 1, 2008